CMS Cloud Computing Policy

Version 1.0

November 12, 2014

Foreword

This *Centers for Medicare & Medicaid Services (CMS) Cloud Computing Policy* provides the high-level guidance for CMS Business and Program stakeholders in the use of cloud computing technology services. CMS recognizes the power and capabilities provided by these services, however, they also come with inherent risks, as well as governing federal mandates.

With this policy, we clarify the guidelines and direction for a consistent approach to cloud computing. Actual processes for acquiring, contracting, and implementing these services will be addressed in the Expedited Life Cycle (XLC) and subsequent published cloud-specific documentation.

\s\ 11/21/2014

David Nelson *Date*
Deputy Chief Operating Officer
Chief Information Officer
Centers for Medicare & Medicaid Services

Record of Changes

Number	Date	Author / Owner	Description of Change	CR #

Table of Contents

Introduction

The Centers for Medicare & Medicaid Services (CMS) processes-and-retains one of the largest volumes of data related to health care in the world, and disseminates more data than almost any other federal agency or public company. In our effort to support our federal information technology (IT) reform objectives, we fully embrace the use of cloud computing technology in a measured way that maintains the security and integrity of CMS systems and data.

While cloud computing is not a new model for processing data and information, it is evolving at a rapid pace. When deployed, the current federal definition of cloud computing could provide CMS with greater operational capacity and flexibility while offering increased agility in developing agency capabilities. CMS supports the use of cloud computing services and components that cost effectively deliver needed efficiencies for our internal and external stakeholders. It is CMS's policy to incorporate cloud computing services, as appropriate, across the agency in compliance with federal and Department regulations for information technology, security, privacy, and confidentiality.

Purpose

The purpose of this policy is to set forth directives concerning the procurement, deployment, and utilization of cloud computing services across the CMS enterprise. This is not a process guide for developing or deploying computing projects at CMS.

Audience

This policy applies to all CMS management, system owners/managers, information owners/stewards, system maintainers, system developers, operators, contracting administrators, technical representatives and administrators. This policy is also applicable to contractors and third parties that support CMS information systems, facilities, communications networks, and information in their work with CMS.

Scope of Policy

This policy governs only new or legacy computing project implementations that are deemed cloud computing solutions. Within CMS, a "cloud computing installation" possesses characteristics consistent with those defined by the National Institute of Standards and Technology (NIST).[1] New and/or legacy computing project implementations undergo standard IT governance reviews as part of the IT lifecycle to ensure appropriate transition to and utilization of cloud computing services across the CMS enterprise. Not all CMS computing deployments are "cloud" installations, and thus, are not subject to this policy.

Definition of "Cloud"

Cloud computing is a *business model* for managing IT infrastructure and assets by:

> *…enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.*

Cloud computing is ***not*** a new architecture, new technology, or even a new methodology. By these standards, to be classified as a "cloud-computing" installation, the service/capability must either consider itself a Cloud or meet at least two of the "five essential" characteristics listed below:

- ***On-demand self-service.*** CMS can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

[1] *The NIST Definition of Cloud Computing*, Special Publication 800-145, National Institute of Standards and Technology, September 2011; and updated 2012.

- ***Broad network access.*** Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick-client platforms (e.g., mobile phones, tablets, laptops, and workstations).
- ***Resource pooling.*** The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.
- ***Rapid elasticity.*** Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
- ***Measured Service.*** Cloud systems automatically control and optimize resource use by leveraging a metering capability[2] at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

CMS can obtain cloud computing services from a Cloud Service Provider (CSP) using three recognized service model arrangements:

- **Software as a Service (SaaS).** The computing capability uses a service provider's applications running on a cloud infrastructure, where CMS would have no control over the infrastructure, network, servers, or operating system used to deliver the software.
- **Platform as a Service (PaaS).** CMS can deploy and control software and applications onto the CSP's computing platform using the programming languages, libraries, services, and tools supported by the CSP. In this instance, CMS does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, or storage, but has control over the deployed applications and configuration settings for the application hosting environment.
- **Infrastructure as a Service (IaaS).** CMS can provision processing, storage, networks, and other fundamental computing resources as necessary to deploy and run any software, which can include operating systems and applications. CMS would not manage or control the underlying cloud infrastructure, but would have control over operating systems, storage, and deployed applications and some limited control of select networking components.

Policy

The CMS Cloud Policy, and subsequent directives, will facilitate our management of data across a large number of dispersed systems, contractors, services, and data centers. This policy provides guidance and direction on the acceptable uses of cloud service providers and cloud computing services. The CMS Cloud Policy comprises the following four directives.

[2] Typically, this is done on a pay-per-use or charge-per-use basis.

1. Permitted Clouds

CMS permits Federal Risk and Authorization Management Program (FedRAMP)-approved cloud Services within the CMS environment which includes both Joint Authorization Board (JAB) provisional Authority to Operate (ATO) and an agency ATO

CMS recognizes there are varying degrees of maturity for cloud services and CSPs. Only FedRAMP-approved cloud services will be considered for acceptable uses of cloud computing installations at CMS. CMS has established the following guidance for consideration of cloud services and cloud computing installations.

a. All Cloud Service Providers must meet the following FedRAMP requirements:

- For cloud-based services and CSPs that may host Personally Identifiable Information (PII)[3] , Protected Health Information (PHI)[4], Electronic PHI (ePHI), or Federal Tax Information (FTI), the CSP shall apply the additional and mandatory security and privacy controls as defined in the *CMS Information Security (IS) Acceptable Risk Safeguards (ARS)*, as amended, in Appendix B, *CMS Minimum Security Requirements (CMSRs) for Moderate Impact Level Data* (available in the IS library at: http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html). CSPs must meet the minimum baseline; the Application should have the ability to meet these controls. A risk based decision must be made if the controls are identified.
- A FedRAMP-Accredited Third-Party Assessment Organization (3PAO) will be used to assess the CSP to determine the extent to which security controls are implemented correctly, operate as intended, and produce the desired outcome with respect to meeting security requirements. A listing of accredited 3PAOs is available at http://www.fedramp.gov/.
- The CSP shall have obtained acceptance of the applicable cloud service by the FedRAMP[5] PMO and available in the FedRAMP Secure Repository within 90 days of award/acquisition.

---

[3] CMS adopts the definition of PII as stated in OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 2007.
[4] PHI is defined in 45 C.F.R. §160.103, available at http://edocket.access.gpo.gov/cfr_2004/octqtr/pdf/45cfr160.103.pdf.
[5] FedRAMP approval is required, throughout the Federal Government, for all CSPs after June 2014, as defined in the December 8, 2011 OMB Memorandum, *Security Authorization of Information Systems in Cloud Computing Environments* (FedRAMP Policy Memo: https://cio.gov/wp-content/uploads/2012/09/fedrampmemo.pdf). CMS expects that CSPs are actively engaged with the FedRAMP approval process at the time bids are submitted (e.g. All required documentation have been completed and submitted to the FedRAMP PMO). CSPs that have not received FedRAMP approval within the 90 day timeframe may be determined to be in breach of contract pending a risk based decision by the CMS CIO.

- Legacy CMS CSPs that are not FedRAMP approved must be reported to the Department of Health and Human Services and Office of Management and Budget as non-compliant systems, and provide justification as to why they are not compliant. [6]
- Legacy CMS CSPs must implement a strategy to becoming FedRAMP compliant within 90 days of the implementation of this policy.

2. CMS Authorization to Operate (ATO)

All cloud service implementations must receive a CMS-issued ATO

All cloud service implementations must have an approved FedRAMP use case[7]. Granting the CMS ATO for use of these installations is at the sole discretion of the CMS Chief Information Officer (CIO). By granting the CMS ATO, the CIO will have considered:

- If the proposed cloud service provider is approved for the applicable use case and in the FedRAMP Secure Repository.
- If the proposed cloud service provider is used by CMS or another agency AND in the process of obtaining FedRAMP approval.

Additionally, the CIO will consider the intended use for the cloud service installation. Appropriate use of cloud technologies is determined by whether the CSP usage will:

- Promote the use of Green IT by reducing the overall energy and real estate footprint of government data centers;
- Reduce the cost of data center hardware, software, and operations;
- Increase the overall IT security posture of the government; and
- Shift IT investments to more efficient computing platforms and technologies.

3. Cloud Use Case

Approved cloud services must comply with their approved use cases, as documented in the CMS Cloud Services Repository

CMS will adhere to existing information security and privacy laws and regulations. Accordingly, the proposed use of the cloud service must be clearly articulated in preparation for review.

---

[6] See OMB M-13-09, Fiscal Year 2013 PortfolioStat Guidance: Strengthening Federal IT Portfolio Management http://www.whitehouse.gov/sites/default/files/omb/memoranda/2013/m-13-09.pdf

[7] FedRAMP "Use Cases" are discussed in detail in the FedRAMP "Guide to Understanding FedRAMP", which is available in the documentation library at http://cloud.cio.gov/fedramp/templates.

The Cloud Services Repository will report the following information for each approved cloud installation:

- Use Case – describing how the service will be used
- Data Categorization [8]– describing how and where data will be stored in this cloud solution
- Risk Factors – describing what risks exist with respect to operating or maintaining agency data

4. FedRAMP Approval

CMS may sponsor Cloud Service Providers through the FedRAMP approval process

If the CSP is not FedRAMP approved and is deemed essential to the applicable business, CMS may choose to assist and/or support the CSP through the FedRAMP approval process. This approval process requires considerable commitment in time, staffing, and funding from the business component as well as the CSP on a continual basis. The CMS CIO exercises the ultimate authority for approving CMS's sponsorship of a cloud service installation through the FedRAMP approval process. The CIO's approval will consider:

- Whether the desired CSP service is already available from an existing FedRAMP- or CMS-approved CSP;
- Whether the business and financial risk is acceptable to commit CMS resources to a CSP that is not yet approved within the FedRAMP process; and
- Whether FedRAMP or CMS will provide continuous monitoring of the Cloud Service Providers program on behalf of any and all other federal agencies that may use this CSP in the future, as required by FedRAMP.

Roles and Responsibilities

Responsibilities for adhering to this policy are role based. The relevant operational and oversight responsibilities are as follows:

- CMS CIO – reviews, adjudicates, and tracks cloud installation service providers and cloud installation use cases; certifies and authorizes systems for use at CMS.
- Contracting Officer's Representatives (COR), ensure that the services are purchased in accordance with federal and CMS policies, and monitor performance of the services over the life of the contract.

[8] CMS Data Categorization is described in the CMS *Risk Management Handbook (RMH)* available at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html.

- Business Owners, System Developers, and System Maintainers – adhere to CMS and federal systems development and operations guidelines.
- General Services Administration (GSA) – maintains the FedRAMP repository of certified Cloud Service Installations and Cloud Service Providers.
- Chief Information Security Officer – Oversight and guidance of FedRAMP ATO approval process within the CMS environment

Governance

Normal governance activities will drive the review and ATO granting process. This process includes reviews by the CMS Information Technology Investment Review Board (ITIRB) and Technical Review Board (TRB) as noted in the Expedited Life Cycle (XLC) and Technical Reference Architecture (TRA) documents. In the course of governance reviews, each project must demonstrate its ability to answer questions of intended use for the cloud installation and the presence of the CSP or Cloud Service Installation in the FedRAMP secure repository.

The CIO grants system-specific (and thus cloud service installation) ATOs on recommendation by the CISO. For all recurring projects that use cloud service installations, CMS will conduct an Annual Operational Assessment (AOA). The AOA will occur at a time specified by OIS or at the direction of the specific Executive Steering Committee with oversight responsibility for the project containing the cloud installation.

Effective Dates

This policy is effective immediately.

Approval

This policy is approved by David Nelson, Chief Information Officer, Centers for Medicare & Medicaid Services.

Related Process References

- The CMS Expedited Life Cycle (XLC): http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/XLC/index.html
- Information about the CMS Technical Reference Architecture (TRA): http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/Technical-Reference-Architecture-Standards/index.html

- *CMS Information Security (IS) Acceptable Risk Safeguards (ARS)*: http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html
- CMS *Risk Management Handbook (RMH)*, Volumes I, II, & III: http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html
- GSA – FedRAMP *Concept of Operations (CONOPS)*: www.gsa.gov/graphics/staffoffices/FedRAMP_CONOPS.pdf
- Office of Management and Budget (OMB) Memorandum, Security Authorization of Information Systems in Cloud Computing Environments: https://cio.gov/wp-content/uploads/2012/09/fedrampmemo.pdf
- *25 Point Implementation Plan to Reform Federal Information Technology Management*, Vivek Kundra, U.S. CIO, December 9, 2010: http://www.dhs.gov/sites/default/files/publications/digital-strategy/25-point-implementation-plan-to-reform-federal-it.pdf
- *The Federal Cloud Computing Strategy:* https://cio.gov/wp-content/uploads/downloads/2012/09/Federal-Cloud-Computing-Strategy.pdf
- *Information about the CMS Technical Reference Architecture (TRA):* http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/Technical-Reference-Architecture-Standards/index.html

Acronyms

3PAO	Third-Party Assessment Organization
AOA	Annual Operational Assessment
ARS	Acceptable Risk Safeguards
ATO	Authority To Operate
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COR	Contracting Officer's Representative
CSP	Cloud Service Provider
ePHI	Electronic Protected Health Information
FedRAMP	Federal Risk Authorization and Management Program
FTI	Federal Tax Information
GSA	General Services Administration
GTR	Government Technical Representative
HHS	Department of the Health and Human Services
IaaS	Infrastructure as a Service
IS	Information Security
ITIRB	Information Technology Investment Review Board
JAB	Joint Authorization Board
NIST	National Institute of Standards and Technology
OIS	Office of Information Services
OMB	Office of Management and Budget
PaaS	Platform as a Service
PHI	Protected Health Information
PII	Personally Identifiable Information
PMO	Program Management Office
RMH	Risk Management Handbook
SaaS	Software as a Service
TRA	Technical Reference Architecture
TRB	Technical Review Board
XLC	Expedited Life Cycle